eFOCUS
Outsourcing kybernetickej bezpečnosti

SLA vo verejnej správe (B2G): kam smeruje dobrá prax?

JUDr. Tomáš Klinka, advokát a patentový zástupca

Nový Smokovec, 16.04.2026

Čo dnes preberieme

01

Reakčné a nápravné časy

Ako ich definovať tak, aby boli reálne vynútiteľné aj pri incidente.

02

KPI a reporting

Kde vznikajú najčastejšie chyby pri nastavovaní metrík a reportingu.

03

Kontrolné práva objednávateľa

Aké práva si má objednávateľ ponechať aj pri plnom outsourcingu.

04

Kontinuita a vendor lock-in

Ako zabezpečiť kontinuitu – kódy, know-how, súčinnosť, komunikácia, cena.

05

Nové „desatoro" ITVS

Návrh novely zákona o ITVS v NRSR a jeho dopad na IT zmluvy.

06

Výklad obchodných zmlúv

Ako sa vykladajú obchodné zmluvy a aký to má dopad na SLA. Praktické príklady.

KAPITOLA 1

Reakčné a nápravné časy

Ako ich definovať tak, aby boli reálne vynútiteľné

Kľúčový problém: „best effort" SLA

Čo je zlé na „best effort"?

SLA formulovaná ako „best effort" bez merateľného momentu vzniku incidentu a bez dôkaznej väzby je **nevynútiteľná** . Best effort prichádza do úvahy len výnimočne – v najmenej závažných (bežných) incidentoch.

Konštrukčná zásada: moment vzniku incidentu

Incident nevzniká „keď si ho dodávateľ prečíta". Vzniká:

- doručením do service desku,
- automatickým monitoringom,
- detekciou SIEM,
- oznámením tretej strany (NBÚ, CSIRT).

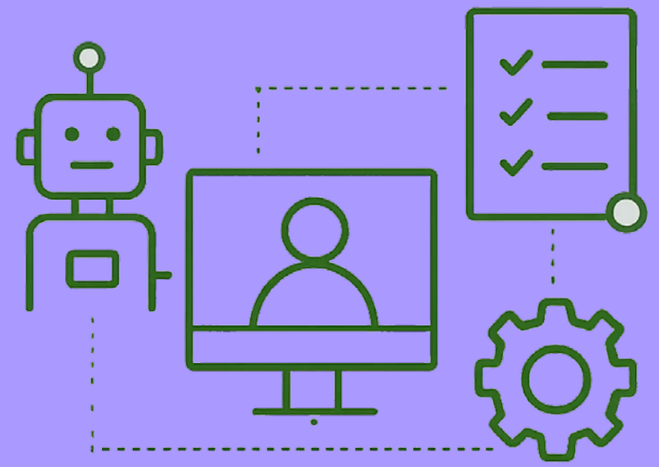
SLA musí obsahovať **fikciu vzniku incidentu** : *„Incident sa považuje za oznámený okamihom jeho zaevidovania v systéme…"*

⚠ Bez presnej definície momentu vzniku incidentu nie je možné merať ani vymáhať žiadny reakčný čas.

Kto a ako nahlasuje

Zmluva musí jednoznačne určiť, kto je oprávnený nahlásiť incident, akým kanálom a čo sa považuje za okamih nahlásenia. Nižšie je príklad typickej klauzuly zo servisnej zmluvy.

PRÍKLAD: Nahlasovanie incidentov – oprávnené osoby, kanály (e-mail, portál, telefón) a fikcia doručenia sú definované v prílohe zmluvy. Systém automaticky generuje potvrdenie s časovou pečiatkou, ktorá je záväzná pre výpočet reakčného času.



SERVICE DESK

KTO a AKO nahlasuje (príklad):

6.1 Požiadavky na riešenie Incidentov je Objednávateľ povinný nahlasovať prostredníctvom Informačného systému pre správu požiadaviek. Zoznam osôb oprávnených pre nahlásenie požiadavky na riešenie Incidentu zo strany Objednávateľa a ich kontaktné údaje sa Oprávnená osoba Objednávateľa zaväzuje dodať Poskytovateľovi v písomnej forme do 5 pracovných dní od uzavretia Zmluvy bez požiadania; každú zmenu týchto osôb je Objednávateľ povinný bezodkladne nahlásiť Poskytovateľovi písomne (e-mailom).

6.2 Poskytovateľ je povinný príjem požiadavky Objednávateľa na riešenie Incidentu bezodkladne potvrdiť prostredníctvom ServiceDesk, v opačnom prípade je Objednávateľ povinný využiť iný spôsob kontaktovania Poskytovateľa (najmä telefonicky). V prípade ak Poskytovateľ bezodkladne nepotvrdí Objednávateľovi príjem požiadavky ani po využití iného spôsobu kontaktovania Poskytovateľa, platí, že požiadavka bola zo strany Poskytovateľa prijatá.

Odkedy beží čas

PRÍKLAD: Čas začína plynúť okamihom zaevidovania incidentu v systéme service desku, nie okamihom jeho prečítania alebo potvrdenia zo strany dodávateľa. Výluky (napr. víkendy pri nižších prioritách) musia byť explicitne vymenované.

Reakčný čas ≠ začiatok riešenia

Reakčný čas treba definovať ako tri samostatné míľniky:

1. Acknowledgement time

Potvrdenie prevzatia / fikcia prevzatia

2. Response time

Začatie riešenia – kvalifikované posúdenie a zahájenie mitigácie

3. Mitigation time

Stabilizácia služby (+ pri bezpečnosti: Containment a Forensic support)

POZOR na skratky: TTR (Time To Respond / Time To Resolve), TTA (Time To Attend), TTF (Time To Fix), TTC (Time To Complete) – rôzni dodávatelia používajú rovnaké skratky s rôznym významom. Vždy definujte obsah, nie len skratku.

ODKEDY beží čas (príklad)

6.6 Poskytovateľ sa zaväzuje dodržať pri riešení Incidentov reakčné doby:

a) pri **Vážnych incidentoch** sa Poskytovateľ zaväzuje začať so zásahom najneskôr **do 1 hodiny** v rámci základného časového pokrytia (t.j. od 8.00 do 17:00 hod. od pondelka do piatku s výnimkou štátnych sviatkov a dní pracovného pokoja) od nahlásenia Vážneho incidentu Objednávateľom alebo jeho zistenia Poskytovateľom,

b) pri **Kritických incidentoch** sa Poskytovateľ zaväzuje začať so zásahom najneskôr **do 1 hodiny** od nahlásenia Kritického incidentu Objednávateľom alebo jeho zistenia Poskytovateľom bez ohľadu na základný rámec časového pokrytia,

c) pri **Bežných incidentoch** sa Poskytovateľ zaväzuje začať so zásahom najneskôr **do 2 hodín** v rámci základného časového pokrytia (t.j. od 8.00 do 17:00 hod. od pondelka do piatku s výnimkou štátnych sviatkov a dní pracovného pokoja) od nahlásenia Bežného incidentu Objednávateľom alebo jeho zistenia Poskytovateľom,

d) pri **Bezpečnostných incidentoch** sa Poskytovateľ zaväzuje začať so zásahom najneskôr **do 1 hodiny** od nahlásenia Bezpečnostného incidentu Objednávateľom alebo jeho zistenia Poskytovateľom bez ohľadu na základný rámec časového pokrytia a bez ohľadu na to, či k Bezpečnostnému incidentu došlo pri riadnom fungovaní Informačného systému alebo v súvislosti s Vážnym incidentom alebo Kritickým incidentom.

Nápravný čas a workaround

Nápravný čas (resolution) vo verejnej správe

Musí byť viazaný na **funkčný stav služby** , nie na „uzavretie ticketu". Oddelene sa definuje:

- **Dočasné riešenie (workaround)** – služba je obnovená náhradným spôsobom,
- **Trvalá náprava** – príčina incidentu je definitívne odstránená.

PRÍKLAD (Trvalé riešenie vs. W orkaround): Zmluva rozlišuje „dočasné obnovenie prevádzky" a „trvalé odstránenie príčiny". Každý míľnik má vlastný termín a vlastnú sankciu. BI = KI: Business Impact sa rovná Kritickosti Incidentu – klasifikácia musí byť objektívna a vopred dohodnutá.

Definície – PRÍKLAD

Príklad typických definícií zo servisnej zmluvy zahŕňa:

- Incident – neplánované prerušenie alebo zníženie kvality IT služby,
- Kritický incident (P1) – výpadok produkčného systému s dopadom na všetkých používateľov,
- Vysoká priorita (P2) – čiastočný výpadok s obmedzeným dopadom,
- Stredná priorita (P3) – degradácia výkonu bez výpadku,
- Nízka priorita (P4) – kozmetické chyby, požiadavky na zmenu.

Každá priorita má vlastné reakčné, mitigačné a nápravné časy.

TRVALÉ RIEŠENIE alebo WORKAROUND?

6.7 Poskytovateľ sa zaväzuje v súčinnosti s technickou podporou Objednávateľa nahlásené alebo zistené Incidenty riešiť až do:

a) ich trvalého vyriešenia, alebo ak nie je objektívne možné Incident bez zbytočného odkladu trvale vyriešiť, do

b) zabezpečenia ich neutralizácie prostredníctvom dočasného režimu funkčnosti Informačného systému (funkcia a plánovaná použiteľnosť Informačného systému je odlišná od požiadaviek a funkčnej špecifikácie, avšak táto odlišnosť nemá podstatný vplyv na pôvodne plánované využitie Informačného systému) vytvorením náhradného postupu alebo dočasného riešenia.

6.8 **Poskytovateľ sa zaväzuje v zmysle bodu 6.7 Zmluvy vyriešiť (Doba trvalého vyriešenia):**

a) **Vážny incident** najneskôr do 6 hodín,

b) **Kritický incident** najneskôr do 4 hodín,

c) **Bežný incident** najneskôr do 24 hodín,

d) **Bezpečnostný incident** najneskôr do 4 hodín.

BI= KI (príklad)

6.5 Bezpečnostné incidenty sa vždy považujú za Kritické incidenty, a to aj v prípade, ak závažnosť Incidentu nemá vplyv na obvyklú funkčnosť Systému, alebo ak nedosahuje intenzity Kritického incidentu.

DEFINÍCIE (príklad)

i. „**Bezpečnostný incident**“ je akýkoľvek spôsob narušenia bezpečnosti Informačného systému, ako aj akákoľvek bezpečnostná udalosť (udalosť, ktorá bezprostredne ohrozila aktívum alebo činnosť Objednávateľa), akékoľvek porušenie bezpečnostnej politiky Objednávateľa a pravidiel súvisiacich s bezpečnosťou informačných systémov verejnej správy. Bezpečnostný incident môže i nemusí prebiehať súčasne s Bežným incidentom alebo Kritickým incidentom. Pokiaľ nie je stanovené inak, platia pre povinnosti Poskytovateľa pri riešení Bezpečnostného incidentu ustanovenia o Kritickom incidente.

ii. „**Vážny incident**“ je incident, ktorý sa prejavuje výpadkom fungovania jednotlivých častí Informačného systému alebo ich funkčnosti, pričom neobmedzuje použitie Informačného systému ako celku alebo jeho podstatných častí. Za Vážny incident sa považujú aj všetky ostatné incidenty, ktoré nespĺňajú definíciu Kritického incidentu.

iii. „**Kritický incident**“ je havária/incident, ktorý sa prejavuje výpadkom Systému ako celku, pri ktorom nie je možné použiť ani jednu jeho časť, alebo jeho výpadkom časti Systému, ktorá obmedzuje použitie Systému v podstatnom rozsahu. Odstránenie Incidentu nie je možné dočasne zabezpečiť náhradným riešením Poskytovateľa ani organizačným opatrením Objednávateľa navrhnutého Poskytovateľom. Za kritický sa považuje incident, ktorý sa prejavuje plošne voči aspoň 20 % interným a externým používateľom Systému, je vyvolávaný opakovane alebo má trvalý charakter, a/alebo spôsobuje nepoužiteľnosť celého Systému na stanovený účel.

iv. „**Bežný incident**“ je incident, ktorý nie je Kritický incident, Vážny incident ani Bezpečnostný incident, pričom sa prejavuje tým, že znemožňuje a/alebo obmedzuje používanie Informačného systému, jeho funkčností alebo služieb z hľadiska koncového používateľa. Odstránenie Incidentu je možné dočasne zabezpečiť náhradným riešením Poskytovateľa alebo organizačným opatrením Objednávateľa navrhnutého Poskytovateľom, a to v lehote stanovenej pre náhradné riešenie.

Vynútiteľnosť a sankčný mechanizmus

Podmienky vynútiteľnosti SLA

Ak má byť SLA vynútiteľné, musia byť splnené tieto podmienky:

- Existuje **objektívne merateľný log** ,
- zdroj merania nie je len dodávateľ,
- je definovaný **sporový mechanizmus** merania.

Štandard: meranie zo systému objednávateľa alebo spoločného nástroja, auditovateľné logy, **zákaz jednostranného uzatvorenia incidentu dodávateľom** .

Sankčný mechanizmus

Bez sankcií SLA nie je SLA. Vo verejnej správe:

- Zmluvná pokuta za nedodržanie reakčného času,
- service credit za dostupnosť,
- právo na eskaláciu a step-in,
- možnosť kvalifikovať opakované porušenie ako **podstatné porušenie zmluvy** .

PRÍKLAD (Zmluvné pokuty): Pokuta za nedodržanie reakčného času P1 = X EUR/hodinu. Service credit za dostupnosť pod 99,5 % = Y % z mesačného paušálu. Opakované porušenie (3× za 6 mesiacov) = podstatné porušenie zmluvy s právom odstúpenia.

ZMLUVNÉ POKUTY (príklad)

20. **SANKCIE A ZMLUVNÉ POKUTY ZA INCIDENTAMI A VADAMI**

20.1 V prípade, ak je Poskytovateľ v omeškaní s riešením Incidentu podľa čl. 6 Zmluvy alebo odstránením Vady podľa čl. 8 Zmluvy, je Objednávateľ oprávnený požadovať od Poskytovateľa zmluvnú pokutu vo výške:

a) pri omeškaní s riešením Kritického Incidentu (Vady) alebo Bezpečnostného Incidentu (Vady) 10 % z ceny za Paušálne služby podľa bodu 10.1 Zmluvy a to za každú začatú hodinu omeškania od uplynutia doby stanovenej na vyriešenie Kritického Incidentu (Vady) alebo Bezpečnostného Incidentu (Vady) podľa čl. 6 Zmluvy.

b) pri omeškaní s riešením Vážneho Incidentu (Vady) 1 % z ceny za Paušálne služby podľa bodu 10.1 Zmluvy a to za každú začatú hodiFdonu omeškania od uplynutia doby stanovenej na vyriešenie Vážneho Incidentu (Vady) podľa čl. 6 Zmluvy, najviac však 30% z ceny za Paušálnej služby podľa bodu 10.1 Zmluvy.

c) pri omeškaní s riešením Bežného Incidentu (Vady) 0,5 % z ceny za Paušálne služby podľa bodu 10.1 Zmluvy a to za každFú začatú hodinu omeškania od uplynutia doby stanovenej na vyriešenie

Bežného Incidentu (Vady) podľa čl. 6 Zmluvy, najviac však 30% z ceny za Paušálnej služby podľa bodu 10.1 Zmluvy.

SERVIS CREDIT za dostupnosť (príklad)

20.3 V prípade, ak Poskytovateľ nedodržiava úroveň dostupnosti produkčného prostredia IS podľa Prílohy č. 4 Zmluvy, je Objednávateľ oprávnený požadovať od Poskytovateľa zmluvnú pokutu vo výške pomernej časti ceny za Paušálne služby podľa bodu 10.1 Zmluvy (Paušálny poplatok) pripadajúcej na chýbajúce percentá do hodnoty dohodnutej úrovne dostupnosti produkčného prostredia IS podľa Prílohy č. 4 Zmluvy.

SERVIS CREDIT za dostupnosť (príklad)

Paušálny poplatok v nasledujúcom mesiaci sa poníži o zmluvnú pokutu podľa bodu 20.3 Zmluvy vyčíslenú podľa uvedených parametrov pomerne k výške Paušálneho poplatku.

Výnimky z výpočtu času nedostupnosti

Do výpočtu nedostupnosti D pre účely zníženia paušálnej odmeny sa nezapočítava:

- čas nedostupnosti spôsobený nedostupnosťou iného ISVS napr. GovNet,
- čas nedostupnosti spôsobený okolnosťami vyššej moci,
- čas nedostupnosti spôsobený okolnosťami na strane Objednávateľa,
- čas nedostupnosti spôsobený okolnosťami tretích strán vylučujúcimi zodpovednosť,
- čas nedostupnosti spôsobený výpadkami HW komponentov alebo infraštruktúry, systému ÚPVS z dôvodu ich zastaranosti, nedostatočnej kapacity, nedostatočnej podpory zo strany výrobcu, alebo iného dôvodu, ktorý nepatrí do zodpovednosti Poskytovateľa,
- čas nedostupnosti spôsobený prekročením kapacity systému doručovania garantovaného Poskytovateľom zo strany používateľov alebo integrovaných IS

PODSTATNÉ PORUŠENIE (príklad)

22.5 Podstatným porušením zmluvnej povinnosti podľa tejto Zmluvy na strane Poskytovateľa je:

a) nepravdivosť niektorého z vyhlásení Poskytovateľa podľa čl. 3 Zmluvy,

b) nepredloženie poistnej zmluvy (poistky) podľa bodu 3.4 Zmluvy,

c) Poskytovateľ opakovane (3x a viac) poskytuje Plnenia s vadami, Plnenia nie sú poskytované v požadovanej kvalite a požadovanej úrovni poskytovania služieb,

d) Poskytovateľ nedodržiava úroveň dostupnosti Prevádzkového prostredia IS podľa Prílohy č. 4 Zmluvy a táto úroveň dostupnosti je v stanovenom mesačnom období menšia ako 98,5%,

e) Poskytovateľ poruší povinnosti vzťahujúce sa k subdodávateľom podľa čl. 19 Zmluvy,

f) porušenie ktorejkoľvek z povinností Zhotoviteľa vzťahujúcej sa k ochrane Dôverných informácií podľa čl. 13 Zmluvy,

g) porušenie ktorejkoľvek z povinností Zhotoviteľa pri výkone kontroly alebo auditu,

h) porušenie ktorejkoľvek z povinností Zhotoviteľa týkajúcej sa bezpečnosti podľa čl. 14 Zmluvy,

i) opakované (3x a viac) porušovanie inej povinnosti Poskytovateľa podľa tejto Zmluvy.

Na zamyslenie:

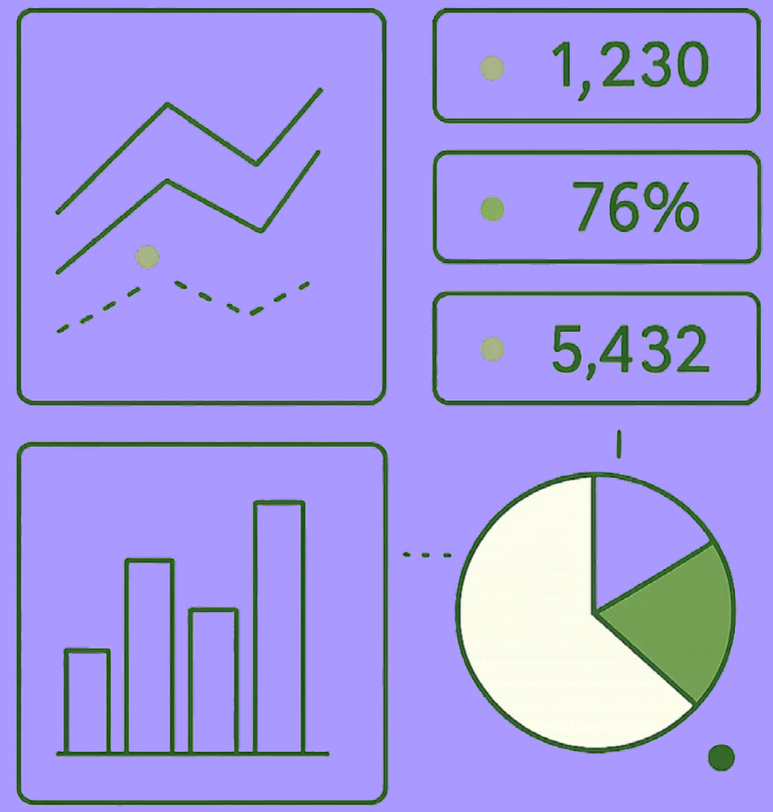
Potrebujete odstúpenie, ak môžete Servisnú zmluvu rýchlo vypovedať?

KAPITOLA 2

KPI a reporting

„What gets measured gets managed“

Peter Drucker (1956)



Päť chýb pri nastavovaní KPI

KPI bez právneho následku

Metriky bez väzby na sankciu, remediation plan ani eskaláciu sú nevynútiteľné.

KPI meria dodávateľ sám sebe

Jediný zdroj dát je dodávateľ – zásadný konflikt záujmov.

KPI sú agregované

Mesačný súhrn môže zakryť kritický výpadok v pracovný deň.

KPI nereflektujú architektúru

„Štandardné čísla" bez väzby na realitu vedú k permanentnému porušovaniu.

KPI sledujú len dostupnosť

Systém môže byť „up", ale pomalý, chybový či nefunkčný.

Správny model KPI: 4 vrstvy

A. Availability KPI

Uptime, výpadky, plánované odstávky

B. Performance KPI

Response time, throughput, latencia

C. Service KPI

Reakčný čas ticketov, nápravný čas, first time fix rate

D. Governance KPI

Včasnosť reportov, kvalita dokumentácie, plnenie CAPA

Každý KPI musí mať

- Definíciu a vzorec výpočtu
- Zdroj dát a periodicitu
- Zodpovednú osobu
- Výluky a spôsob validácie

Bez týchto atribútov KPI nefunguje

KPI bez definície zdroja dát, vzorca a zodpovednej osoby je nevymáhateľné a pri audite neobhájiteľné.

Právne väzby KPI a reporting

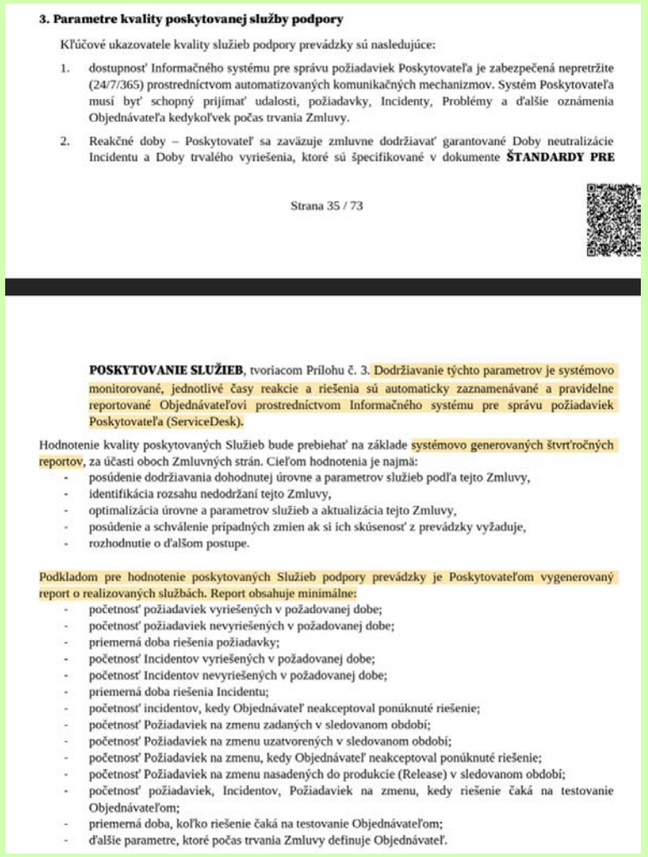
Právna väzba každého KPI

- Service credit
- Zmluvná pokuta
- Povinný remediation plan
- Eskalácia na riadiacu úroveň
- Právo objednávateľa auditovať
- Kvalifikované porušenie pri opakovanom neplnení

Mesačný report musí obsahovať

1. Tabuľku všetkých KPI s hodnotami a statusom (splnené/nesplnené)
2. Per-incident prehľad s časmi, klasifikáciou a root cause
3. Trend sekciu
4. Management summary na 1 stranu bez technického žargónu

KPI a reporting (príklad)



3. Parametre kvality poskytovanej služby podpory

Kľúčové ukazovatele kvality služieb podpory prevádzky sú nasledujúce:

1. dostupnosť Informačného systému pre správu požiadaviek Poskytovateľa je zabezpečená nepretržite (24/7/365) prostredníctvom automatizovaných komunikačných mechanizmov. Systém Poskytovateľa musí byť schopný prijímať udalosti, požiadavky, Incidenty, Problémy a ďalšie oznámenia Objednávateľa kedykoľvek počas trvania Zmluvy.
2. Reakčné doby – Poskytovateľ sa zaväzuje zmluvne dodržiavať garantované Doby neutralizácie Incidentu a Doby trvalého vyriešenia, ktoré sú špecifikované v dokumente **ŠTANDARDY PRE**

POSKYTOVANIE SLUŽIEB, tvoriacom Prílohu č. 3. Dodržiavanie týchto parametrov je systémovo monitorované, jednotlivé časy reakcie a riešenia sú automaticky zaznamenávané a pravidelne reportované Objednávateľovi prostredníctvom Informačného systému pre správu požiadaviek Poskytovateľa (ServiceDesk).

Hodnotenie kvality poskytovaných Služieb bude prebiehať na základe systémovo generovaných štvrťročných reportov, za účasti oboch Zmluvných strán. Cieľom hodnotenia je najmä:

- posúdenie dodržiavania dohodnutej úrovne a parametrov služieb podľa tejto Zmluvy,
- identifikácia rozsahu nedodržaní tejto Zmluvy,
- optimalizácia úrovne a parametrov služieb a aktualizácia tejto Zmluvy,
- posúdenie a schválenie prípadných zmien ak si ich skúsenosť z prevádzky vyžaduje,
- rozhodnutie o ďalšom postupe.

Podkladom pre hodnotenie poskytovaných Služieb podpory prevádzky je Poskytovateľom vygenerovaný report o realizovaných službách. Report obsahuje minimálne:

- početnosť požiadaviek vyriešených v požadovanej dobe;
- početnosť požiadaviek nevyriešených v požadovanej dobe;
- priemerná doba riešenia požiadavky;
- početnosť Incidentov vyriešených v požadovanej dobe;
- početnosť Incidentov nevyriešených v požadovanej dobe;
- priemerná doba riešenia Incidentu;
- početnosť incidentov, kedy Objednávateľ neakceptoval ponúknuté riešenie;
- početnosť Požiadaviek na zmenu zadaných v sledovanom období;
- početnosť Požiadaviek na zmenu uzatvorených v sledovanom období;
- početnosť Požiadaviek na zmenu, kedy Objednávateľ neakceptoval ponúknuté riešenie;
- početnosť Požiadaviek na zmenu nasadených do produkcie (Release) v sledovanom období;
- početnosť požiadaviek, Incidentov, Požiadaviek na zmenu, kedy riešenie čaká na testovanie Objednávateľom;
- priemerná doba, koľko riešenie čaká na testovanie Objednávateľom;
- ďalšie parametre, ktoré počas trvania Zmluvy definuje Objednávateľ.

REPORT ako výkaz (príklad)

Report (výkaz) k poskytnutým službám

Minimálne obsahové náležitosti reportu pre službu riešenia Incidentov/Problémov:

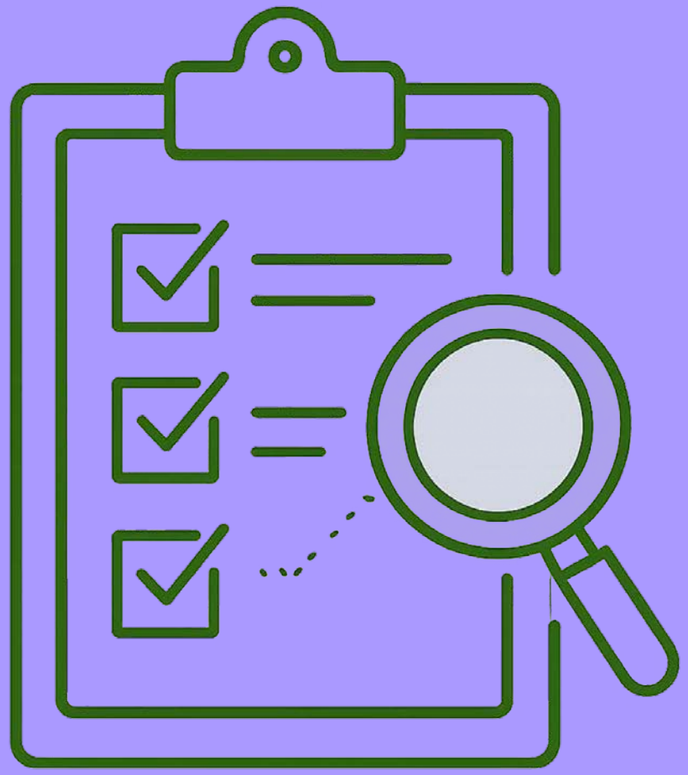
a) jednoznačný identifikátor Incidentu/Problému
b) názov Incidentu/ Problému
c) zoznam riešiteľov
d) skutočné lehoty jednotlivých plnení

Minimálne obsahové náležitosti reportu pre službu profylaktiky:

a) zoznam dokumentov z profylaktických činností s označením jedinečnej verzie
b) obdobie, na ktoré sa vzťahuje výkon z profylaktickej činností
c) autor dokumentu za Poskytovateľa
d) dátum akceptácie jednotlivých dokumentov
e) vlastník dokumentu za VO, ktorý akceptoval príslušný dokument

Minimálne obsahové náležitosti reportu pre službu riešenia Bezpečnostných incidentov (v zmysle požiadaviek Vyhlášky č. 362/2018 Z. z., par. 2):

a) jednoznačný identifikátor Incidentu
b) názov Bezpečnostného incidentu
c) kontaktné údaje osoby, ktorá Bezpečnostný incident nahlásila
d) skutočné lehoty jednotlivých plnení
e) časové údaje priebehu Bezpečnostného incidentu
f) detailný opis priebehu Bezpečnostného incidentu
g) rozsah vzniknutých škôd z dôvodu Bezpečnostného incidentu
h) konkrétny popis všetkých zasiahnutých aktív
i) vplyv Bezpečnostného incidentu na poskytovanú službu/IS/APV/Modul
j) stav riešenia Bezpečnostného incidentu
k) vykonané nápravné opatrenia
l) popis následkov Bezpečnostného incidentu
m) zoznam riešiteľov



KAPITOLA 3

Minimálne práva objednávateľa

Aké kontrolné práva si má objednávateľ ponechať aj pri plnom outsourcingu

Štyri piliere kontrolných práv objednávateľa

A. Audit

Objednávateľ musí mať právo na **interný audit** (vlastný tím), **externý audit** (nezávislý audítor), **regulatorný audit** (NBÚ, ÚVO, NKÚ) a **subdodávateľský audit** – právo auditovať aj subdodávateľov dodávateľa. Rozsah, frekvencia a podmienky musia byť explicitne zmluvne zakotvené.

B. Prístup k dátam

Objednávateľ musí mať zaručený prístup k **logom**, **SIEM** (bezpečnostné udalosti), **konfiguráciám** a **dátam**. Prístup musí byť priebežný (nie len na požiadanie) a nesmie byť podmienený súhlasom dodávateľa.

C. Step-in právo

Právo objednávateľa prevziať kontrolu nad službou pri: **incidente** (kritický výpadok), **SLA zlyhaní** (opakované neplnenie) a **ohrození verejného záujmu** (aspoň príkladmo definované). Step-in musí byť procesne popísaný – kto, ako, za akých podmienok.

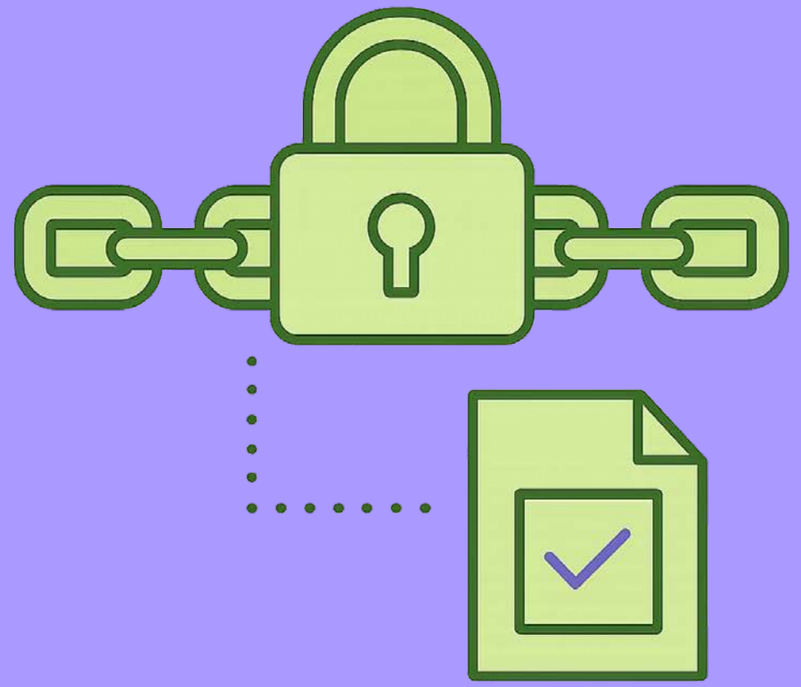
D. Subdodávatelia

Zmluva musí riešiť: **schvaľovanie** subdodávateľov objednávateľom, **flow-down** zmluvných povinností (SLA, bezpečnosť, GDPR) na subdodávateľov a **auditovateľnosť** subdodávateľského reťazca.

KAPITOLA 4

Kontinuita a vendor lock - in

Ako zabezpečiť kontinuitu – kódy, know-how, súčinnosť, komunikácia, cena



Typy vendor lock-in a riešenia

Typy vendor lock-in

- **Staré zmluvy, staré projekty** – historické záväzky bez exit klauzúl,
- **Technologický vendor lock-in** – proprietárne technológie, formáty, skripty,
- **Právny vendor lock-in** – licenčné podmienky bránia prechodu.

⚠ Akékoľvek riešenie vendor lock-in stojí čas a peniaze a môže byť rizikové z hľadiska verejného obstarávania.

Kľúčový faktor: postoj dodávateľa

K riešeniu vendor lock-in je kľúčový postoj dodávateľa. Scenáre sa zásadne líšia podľa toho, či dodávateľ chce alebo nechce dohodu.

Dodávateľ CHCE dohodu

- Transfer poznatkov a práv so školeniami, odovzdaním know-how, zdrojových kódov a licencií = **samostatné plnenie** (možné aj vo fázach), za ktoré má dodávateľ dostať osobitne zaplatené,
- výber nového dodávateľa,
- dojednanie súčinnosti s novým dodávateľom (prechodné obdobie).

Dodávateľ NECHCE dohodu

- Je potrebné sa „odstrihnúť",
- začať budovať s novým dodávateľom nový IS „na zelenej lúke",
- pôvodný dodávateľ bude musieť byť zazmluvnený do nasadenia nového IS.

Príklad zlyhania kontinuity – technologický vendor lock-in

> Dodávateľ servisných služieb po odovzdaní IS objednávateľovi (novému dodávateľovi) pri ukončení servisnej zmluvy zatajil, že na funkčnosť niektorých funkcionalít používa vlastné nástroje (skripty), ktoré netvoria súčasť IS, nie sú súčasťou architektúry riešenia, neboli nikdy odovzdané ani pomenované.

Čo sa stalo

Nový dodávateľ zistil, že niektoré kľúčové funkcionality sú nefunkčné. Reklamácie neprichádzajú do úvahy, nakoľko IS bol pôvodným dodávateľom vytvorený XY rokov dozadu. Nikto od objednávateľa nemal šancu si to všimnúť – navonok IS fungoval, ale len ak ho servisoval pôvodný dodávateľ so svojou externou pomôckou/skriptom.

Kľúčové otázky

- **Kto nesie zodpovednosť** za takýto stav?
- Existuje **„páka"** na pôvodného dodávateľa odovzdať svoju pomôcku (skript), ak je v zmysle klauzuly o súčinnosti povinný „len" poskytnúť súčinnosť?

⊗ Bez zmluvného riešenia nárok objednávateľa na zabezpečenie kontinuity neexistuje! Nestačí „súčinnosť" – musí byť presne vymedzená obsahovo aj rozsahovo.

Zmluvné riešenie kontinuity – ako na to

Obsahové vymedzenie súčinnosti

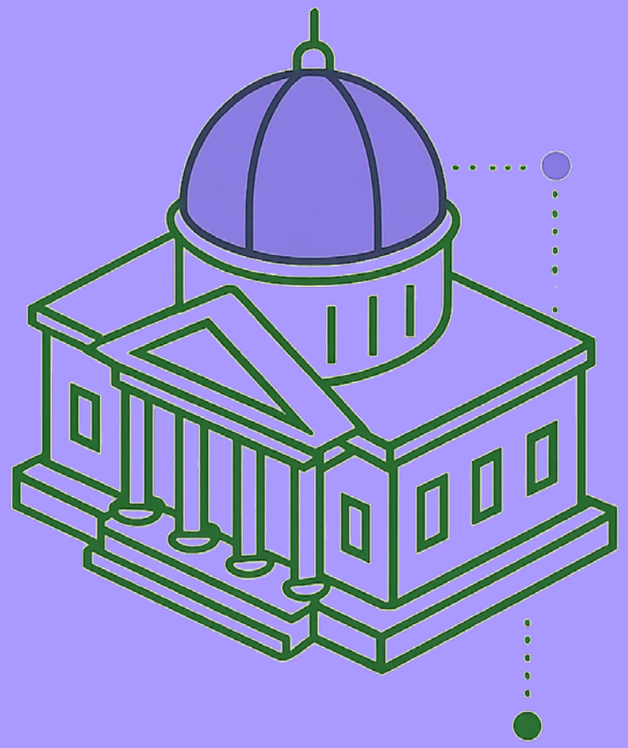
Nestačí „dodávateľ poskytne súčinnosť". Zmluva musí explicitne vymenovať: odovzdanie zdrojových kódov, dokumentácie, architektúry, integračných rozhraní, skriptov, konfigurácií, prístupových údajov, školenia nového dodávateľa.

Rozsahové vymedzenie a cena

Vhodný kompromis: definovať **default rozsah** (napr. XY man-days počas X mesiacov) **v cene** servisnej zmluvy, nad rámec osobitne spoplatnené. Má byť súčinnosť „zdarma" alebo samostatná cenová položka? Oboje má svoje riziká.

Referencie a príklady

Príklad zmluvného riešenia vendor lock-in (2020) – CRZ.gov.sk.
Príklad legislatívneho riešenia vendor lock-in (2025) – slov-lex.sk.
Aktuálne požiadavky zákona o ITVS na IT zmluvu (§ 15).



KAPITOLA 5

Nové „desatoro" v ITVS

Návrh novely zákona o ITVS v NRSR (vládny návrh z dielne MIRRI) – pôvodne plánovaná účinnosť od 1. 3. 2026

§ 15 ods. 2 písm. g) – 10 povinných zmluvných podmienok (1 –5)

Správca je povinný akceptovať len také zmluvné podmienky, podľa ktorých:

Neobmedzené užívanie

Užívanie ITVS správcom, prevádzkovateľom alebo orgánom verejnej moci na výkon ich povinností **nie je obmedzené**.

Voľné použitie IS, dok. a kódu

Dohodnuté spôsoby použitia IS, dokumentácie a zdrojového kódu **neobmedzujú** správcu v možnosti použitia akýmkoľvek spôsobom potrebným pre výkon jeho činnosti.

Súťažný výber dodávateľa

Podmienky použitia **nebránia súťažným spôsobom** z neuzatvoreného okruhu osôb vybrať dodávateľa služieb (podpora, údržba, rozvoj).

Sublicencia pre VS

Je možné udeliť súhlas na použitie IS, dokumentácie a zdrojového kódu **akémukoľvek správcovi alebo orgánu verejnej moci** v rovnakom rozsahu.

Spoluautorské dielo – správca

Ak vznikne dielo spoluautorov, majetkové práva vykonáva **výhradne správca** (vrátane zmien), inak len ak to vedie k vyššej hospodárnosti.

§ 15 ods. 2 písm. g) – 10 povinných zmluvných podmienok (6 –10)

Správca je povinný akceptovať len také zmluvné podmienky, podľa ktorých:

SW tretích strán

Programový prostriedok tretej strany sa môže stať súčasťou IS len so **súhlasom správcu** a ak jeho podmienky neobmedzujú body 1–4.

Databázové práva

Právo použiť databázu a udeliť súhlas na extrakciu alebo reutilizáciu jej obsahu sa **prevedie na správcu** .

Informácie z projektu

Správca je **jediným a výhradným disponentom** so všetkými informáciami zhromaždenými počas projektu a prevádzky.

Súčinnosť pri zmene dodávateľa

Pôvodný dodávateľ poskytne správcovi **úplnú súčinnosť** pri prechode na nového dodávateľa, najmä v oblasti architektúry a integrácie IS.

Súčinnosť pre nový IS

Dodávateľ IS poskytne **inému dodávateľovi** pri vytváraní nového IS súčinnosť potrebnú na riadne vytvorenie a uvedenie do prevádzky (migrácia dát, integrácia IS).

Výklad zmluvy: § 266 Obchodného zákonníka

4 kroky interpretačnej metodiky

1. Subjektívny výklad – skutočný úmysel strany, ak bol druhej strane známy alebo jej musel byť známy
2. Objektívny výklad – význam, ktorý by zmluve prisúdila rozumná osoba v postavení adresáta
3. Ustálená prax – správanie strán počas trvania zmluvy a obchodné zvyklosti
4. Contra proferentem – nejasnosti idú na ťarchu toho, kto formuláciu použil ako prvý

Praktický dosah

- Výkladom nemožno nahrádzať to, čo si strany nedohodli
- Zmluva má odrážať ekonomickú rovnováhu strán
- Ak má byť niečo súčasťou plnenia, musí to byť v zmluve
- Nový Občiansky zákonník tieto princípy ešte systematickejšie kodifikuje

Príklad z praxe: spor o rozsah reportingu

> „Bez explicitnej úpravy v zmluve nie je možné rozsah plnenia spätne rozšíriť výkladom."

Situácia

- Servisná zmluva s paušálnymi službami a jasným vymedzením rozsahu
- Zákazník požadoval „reporting na želanie" ako súčasť plnenia
- Zmluvu formuloval samotný zákazník

Prečo výklad neobstál

- Úmysel nebol pri uzavretí zmluvy komunikovaný
- Nejde o trhový štandard
- Doterajšia prax zmluvných strán to nepotvrdzuje
- Contra proferentem: formuláciu pripravil zákazník → nejasnosť ide na jeho ťarchu

Závery

SLA musí byť merateľné

Presná definícia momentu vzniku incidentu, tri úrovne reakčných časov, oddelenie workaroundu od trvalej nápravy. Bez objektívneho logu a spoločného zdroja pravdy je SLA nevynútiteľné.

KPI bez následku sú dekorácia

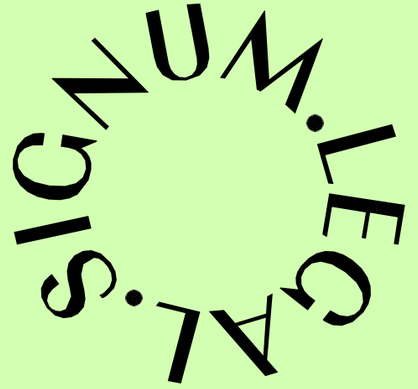
Každý podstatný KPI musí mať právnu väzbu (sankcia, remediation plan, eskalácia). Štyri vrstvy: Availability, Performance, Service, Governance. Reporting musí obsahovať per-incident aj trend dáta.

Kontrolné práva sú nevyhnutné

Audit (interný, externý, regulatorný, subdodávateľský), prístup k logom a SIEM, step-in právo a schvaľovanie subdodávateľov – to sú minimálne práva, ktoré si objednávateľ musí ponechať.

Kontinuita sa musí zmluvne riešiť

Bez zmluvného riešenia nárok na kontinuitu neexistuje. Nové „desatoro" v § 15 ITVS (novela v NRSR) prináša 10 povinných podmienok – od voľného použitia kódu až po súčinnosť pri zmene dodávateľa.



Ďakujem za pozornosť!

SIGNUM legal s.r.o. | JUDr. Tomáš Klinka , advokát a patentový zástupca

SIGNUM.LEGAL